

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Takeshi INADA

Serial No. (unknown)

Filed herewith

ENCRYPTION-DECRYPTION APPARATUS



CLAIM FOR FOREIGN PRIORITY UNDER 35 U.S.C. 119
AND SUBMISSION OF PRIORITY DOCUMENT

Assistant Commissioner for Patents

Washington, D.C. 20231

Sir:

Attached hereto is a certified copy of applicant's corresponding patent application filed in Japan on April 19, 2000, under 2000-118269.

Applicant herewith claims the benefit of the priority filing date of the above-identified application for the above-entitled U.S. application under the provisions of 35 U.S.C. 119.

Respectfully submitted,

YOUNG & THOMPSON

By *Benoit Castel*
Benoit Castel
Attorney for Applicant
Customer No. 000466
Registration No. 35,041
745 South 23rd Street
Arlington, VA 22202
703/521-2297

April 18, 2001

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

J1036 U.S. PRO
09/836172
04/18/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

2000年 4月19日

出 願 番 号

Application Number:

特願2000-118269

出 願 人

Applicant(s):

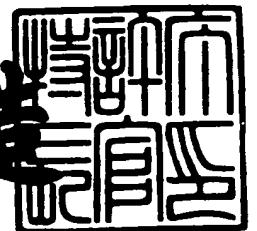
日本電気通信システム株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 2月16日

特許庁長官
Commissioner,
Patent Office

及 川 耕 造



【書類名】 特許願
【整理番号】 01612076
【あて先】 特許庁長官殿
【国際特許分類】 G09C
G06F
H03M
H04L

【発明者】

【住所又は居所】 東京都港区三田一丁目4番28号
日本電気通信システム株式会社内

【氏名】 稲田 剛

【特許出願人】

【識別番号】 000232254

【氏名又は名称】 日本電気通信システム株式会社

【代理人】

【識別番号】 100082935

【弁理士】

【氏名又は名称】 京本 直樹

【電話番号】 03-3454-1111

【選任した代理人】

【識別番号】 100082924

【弁理士】

【氏名又は名称】 福田 修一

【電話番号】 03-3454-1111

【選任した代理人】

【識別番号】 100085268

【弁理士】

【氏名又は名称】 河合 信明

【電話番号】 03-3454-1111

【手数料の表示】

【予納台帳番号】 021566

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9114193

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 暗号復号化装置

【特許請求の範囲】

【請求項 1】 データの暗号化と暗号化データの複合化を行う暗号復号化装置において、暗号化復号化する回路を可変可能な回路装置を用い、前記可変可能な回路装置の回路データを秘密鍵として暗号化複合化を行うことを特徴とする暗号復号化装置。

【請求項 2】 前記可変可能な回路装置の回路データを複数個有し、暗号化複合化を行うための回路データ選択情報から、前記可変可能な回路装置の回路データを選択し供給することで異なるアルゴリズムの暗号化複合化を行うことを特徴とする請求項 1 記載の暗号化復号化装置。

【請求項 3】 入力データを暗号化し暗号化データを出力する送信装置と、前記暗号化データを伝送するネットワーク網と、このネットワーク網を介して伝送されてきて前記暗号化データを入力し、暗号解読を行い復号化した出力データを出力する受信装置とを備え、

前記送信装置は暗号化する可変処理回路と、この可変処理回路に秘密鍵の回路データを出力するリード・オンリー・メモリ（ROM）とを有し、前記受信装置は復号化する可変処理回路と、この可変処理回路に秘密鍵の回路データを出力するリード・オンリー・メモリ（ROM）とを有していることを特徴とする暗号復号化装置。

【請求項 4】 入力データを暗号化し暗号化データを出力する送信装置と、前記暗号化データを伝送するネットワーク網と、このネットワーク網を介して伝送されてきた前記暗号化データを入力し暗号解読を行い復号化した出力データを出力する受信装置とを備え、

前記送信装置は、

前記入力データを決められた指定通りに情報を解析し、デコードして書き換え情報を出力するデータ解析部と；

暗号アルゴリズムを指定する回路データを記憶する複数の ROM と；

前記書き換え情報の指示に従い前記複数の ROM を選択し、選択した ROM か

ら暗号化する回路データを送出するセレクターと；

どのROMを選択するかにより暗号アルゴリズムを指定する前記回路データをもとに、自己の内部回路を書き換え、この内部回路の回路変更が完了すると終了通知信号を出力し、入力保持データを暗号化した暗号化データを前記ネットワーク網に送出する可変処理回路と；

前記終了通知信号を受け、それまで保持していた前記入力データを、暗号化する前記可変処理回路に前記入力保持データとして出力する暗号／復号化データ保持部と；

を有し、

前記受信装置は、

前記ネットワーク網から入力された前記暗号化データを決められた指定通りに情報を解析し、デコードして書き換え情報を出力するデータ解析部と；

暗号アルゴリズムを指定する回路データを記憶する複数のROMと；

前記書き換え情報の指示に従い前記複数のROMを選択し、選択したROMから復号化する回路データを送出するセレクターと；

どのROMを選択するかにより暗号アルゴリズムを指定する前記回路データをもとに、暗号を復号化するため自己の内部回路を書き換え、この内部回路の回路変更が完了すると終了通知信号を出力し、入力保持データの暗号化データを復号化した復号出力データを送出する可変処理回路と；

前記終了通知信号を受け、それまで保持していた前記暗号化データを、復号化する前記可変処理回路に前記入力保持データとして出力する暗号／復号化データ保持部と；

を有することを特徴とする暗号復号化装置。

【請求項5】 入力データを暗号化し暗号化データを出力する送信装置と、前記暗号化データを伝送するネットワーク網と、このネットワーク網を介して伝送されてきた前記暗号化データを入力し暗号解読を行い復号化した出力データを出力する受信装置とを備え、

前記送信装置は、

前記入力データを決められた指定通りに情報を解析し、解析データを出力する

データ解析部と；

暗号アルゴリズムを指定する回路データを保持する複数のデータ回路部と；

前記データ解析部からの前記解析データをもとに選択信号を出力し、回路構成を変更する第 1 の回路データを入力し、第 2 の回路データを生成出力するフィールド・プログラマブル・ゲートアレイ（Field Programmable Gate Array：以下 F P G A と記す）回路データ生成部と；

前記選択信号の指示に従い、複数の回路データを選択し、選択した回路データから暗号化する前記第 1 の回路データを前記 F P G A 回路データ生成部に出力するセレクターと；

前記 F P G A 回路データ生成部が出力する前記第 2 の回路データをもとに、自己の内部回路を書き換え、この内部回路の回路変更が完了すると終了通知信号を出力し、入力保持データを暗号化した暗号化データを前記ネットワーク網に送出する可変処理回路と；

前記終了通知信号を受け、それまで保持していた前記入力データを新たに前記入力保持データとして前記可変処理回路に出力する暗号／復号化データ保持部と；

を有し、

前記受信装置は、

前記ネットワーク網から入力された前記暗号化データを決められた指定通りに情報を解析し、解析データを出力するデータ解析部と；

前記データ解析部からの前記解析データをもとに選択信号を出力し、回路構成を変更する第 1 の回路データを入力し、第 2 の回路データを生成出力する F P G A 回路データ生成部と；

暗号アルゴリズムを指定する回路データを保持する複数のデータ回路部と；

前記選択信号の指示に従い、複数の回路データを選択し、選択した回路データから暗号を復号化する前記第 1 の回路データを前記 F P G A 回路データ生成部に出力するセレクターと；

前記 F P G A 回路データ生成部が出力する前記第 2 の回路データをもとに、暗号を復号化するため自己の内部回路を書き換え、この内部回路の回路変更が完了

すると終了通知信号を出力し、入力保持データの暗号化データを復号化した復号出力データを送出する可変処理回路と；

前記終了通知信号を受け、それまで保持していた前記入力データを新たに前記入力保持データとして前記可変処理回路に出力する暗号／復号化データ保持部と；

を有することを特徴とする暗号復号化装置。

【請求項 6】 前記送信装置が、

前記入力データを入力保持し、終了通知信号を受けると保持していた前記入力データを保持データとして出力する暗号／復号化データ保持部と；

暗号アルゴリズムのデータを記憶するフラッシュROMと；

前記入力データを入力し、第 1 の回路データを前記フラッシュROMに出力し、この第 1 の回路データによりフラッシュROMのデータを書き換え、書き換え終了後前記フラッシュROMからの第 2 の回路データを入力し、自己の内部回路の変更を行い、この内部回路変更後に前記終了通知信号を前記暗号／復号化データ保持部に出力するとともに前記保持データを暗号化した出力データを出力する可変処理回路と；

を有し、

前記受信装置が、

前記暗号化した出力データを入力保持し、終了通知信号を受けると保持していた前記出力データを保持データとして出力する暗号／復号化データ保持部と；

暗号アルゴリズムのデータを記憶するフラッシュROMと；

前記暗号化した出力データを入力し、第 1 の回路データを前記フラッシュROMに出力し、この第 1 の回路データによりフラッシュROMのデータを書き換え、書き換え終了後前記フラッシュROMからの第 2 の回路データを入力し、自己の内部回路の変更を行い、この内部回路変更後に前記終了通知信号を前記暗号／復号化データ保持部に出力するとともに前記保持データの暗号を復号化した出力データを出力する可変処理回路と；

を有することを特徴とする請求項 3、4 又は 5 記載の暗号復号化装置。

【請求項 7】 前記送信装置が、

前記入力データを入力し、回路データを生成出力する回路データ抽出部と；

前記入力データを回路変更終了まで保持し、終了通知信号を受けると、保持していた前記入力データを保持データとして送出する暗号／復号化データ保持部と；

前記回路データにより暗号化する回路変更を行い、回路変更後前記終了通知信号を前記暗号／復号化データ保持部に出力し、変更後の回路構成によって暗号化を行った出力データを出力する可変処理回路と；

を有し、

前記受信装置が、

前記暗号化を行った出力データを入力し、回路データを生成出力する回路データ抽出部と；

前記出力データを回路変更終了まで保持し、終了通知信号を受けると、保持していた前記暗号化を行った出力データを保持データとして送出する暗号／復号化データ保持部と；

前記回路データにより復号化する回路変更を行い、回路変更後前記終了通知信号を前記暗号／復号化データ保持部に出力し、変更後の回路構成によって復号化を行った出力データを出力する可変処理回路と；

を有することを特徴とする請求項 3、4 又は 5 記載の暗号復号化装置。

【請求項 8】 前記送信装置が、

前記入力データを入力保持し、回路変更通知信号を入力すると、保持していた前記入力データを保持データとして出力する暗号／復号化データ保持部と；

暗号化コードを生成するランダム発生器と；

前記入力データが暗号化したいデータであるか復号化したいデータであるかを判定し、暗号化したいデータである場合は、前記ランダム発生器からのデータを有効にするように通知し、復号化したいデータである場合は、暗号鍵を有効にするように通知する解析データを出力するデータ解析部と；

前記解析データの通知に従い第 1 の回路データを生成出力する F P G A 回路データ生成部と；

暗号アルゴリズムを指定する回路データを記憶する複数の R O M と；

前記第 1 の回路データをもとに前記複数の ROM から回路データを取り込み、暗号アルゴリズムを指定する第 2 の回路データを出力するセレクターと；

前記第 2 の回路データを入力すると前記暗号／復号化データ保持部からの前記保持データの送出を止めるように前記回路変更通知信号を出力し、前記第 2 の回路データによって暗号化する自己の内部回路を変更し、変更が終了すると前記回路変更通知信号を停止し、再び前記保持データを送出させ、暗号化した出力データを出力する可変処理回路と；

を有し、

前記受信装置が、

前記暗号化した出力データを入力保持し、回路変更通知信号を入力すると、保持していた前記出力データを保持データとして出力する暗号／復号化データ保持部と；

暗号化コードを生成するランダム発生器と；

前記暗号化した出力データが暗号化したいデータであるか復号化したいデータであるかを判定し、暗号化したいデータである場合は、前記ランダム発生器からのデータを有効にするように通知し、復号化したいデータである場合は、暗号鍵を有効にするように通知する解析データを出力するデータ解析部と；

前記解析データの通知に従い第 1 の回路データを生成出力する F P G A 回路データ生成部と；

暗号アルゴリズムを指定する回路データを記憶する複数の ROM と；

前記第 1 の回路データをもとに前記複数の ROM から回路データを取り込み、暗号アルゴリズムを指定する第 2 の回路データを出力するセレクターと；

前記第 2 の回路データを入力すると前記暗号／復号化データ保持部からの前記保持データの送出を止めるように前記回路変更通知信号を出力し、前記第 2 の回路データによって復号化する自己の内部回路を変更し、変更が終了すると前記回路変更通知信号を停止し、再び前記保持データを送出させ、復号化した出力データを出力する可変処理回路と；

を有することを特徴とする請求項 3、4 又は 5 記載の暗号復号化装置。

【請求項 9】 前記複数の ROM データが、複数のハードウェア化されたデ

ータ回路からのデータであり、前記セレクターが出力する回路データを第 1 の回路データとして前記 F P G A 回路データ生成部に出力し、この F P G A 回路データ生成部が出力する第 2 の回路データを前記可変処理回路に出力することを特徴とする請求項 8 記載の暗号復号化装置。

【請求項 1 0】 前記送信装置が、

前記入力データを入力保持し、回路変更通知信号を入力すると、保持していた前記入力データを保持データとして出力する暗号／復号化データ保持部と；

ある期間毎にセレクター制御信号を生成出力するタイマーと；

暗号アルゴリズムを指定する回路データを記憶する複数の R O M と；

前記セレクター制御信号をもとに前記複数の R O M を選択し暗号化する回路データを取り込み、暗号アルゴリズムを指定する回路データを出力するセレクターと；

前記回路データを受けると前記回路変更通知信号を出力し、前記保持データの送出を停止し、前記回路データをもとに自己の内部の回路構成を変更し、変更が終了すると前記暗号／復号化データ保持部に前記保持データの送出を再開させるべく前記回路変更通知信号を停止し、前記保持データを入力し、変更した内部の回路構成によって暗号化を行い、暗号化した出力データを送出する可変処理回路と；

を有し、

前記受信装置は、

前記暗号化した出力データを入力保持し、回路変更通知信号を入力すると、保持していた前記入力データを保持データとして出力する暗号／復号化データ保持部と；

ある期間毎にセレクター制御信号を生成出力するタイマーと；

暗号アルゴリズムを指定する回路データを記憶する複数の R O M と；

前記セレクター制御信号をもとに前記複数の R O M を選択し暗号化する回路データを取り込み、暗号アルゴリズムを指定する回路データを出力するセレクターと；

前記回路データを受けると前記回路変更通知信号を出力し、前記保持データの

送出を停止し、前記回路データをもとに自己の内部の回路構成を変更し、変更が終了すると前記暗号／復号化データ保持部に前記保持データの送出を再開させるべく前記回路変更通知信号を停止し、前記保持データを入力し、変更した内部の回路構成によって復号化を行い、復号化した出力データを送出する可変処理回路と；

を有することを特徴とする請求項 3、4 又は 5 記載の暗号復号化装置。

【請求項 11】 前記複数の ROM データが、複数のハードウェア化されたデータ回路部からのデータであり、前記ランダム発生器が、ある期間毎にセレクター制御信号を生成出力するタイマーであり、前記セレクターが出力する回路データを第 1 の回路データとして前記 F P G A 回路データ生成部に出力し、この F P G A 回路データ生成部が出力する第 2 の回路データを前記可変処理回路に出力することを特徴とする請求項 8 記載の暗号復号化装置。

【請求項 12】 前記可変処理回路が、フィールド・プログラマブル・ゲートアレイ（F P G A）であることを特徴とする請求項 3、4、5、6、7、8 又は 10 記載の暗号復号化装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は暗号復号化装置に関し、特に暗号解読アルゴリズムを可変できる暗号復号化装置に関する。

【0002】

【従来の技術】

最近、携帯電話など無線を利用した通信技術が急速に発達しており、盗聴などによる通信データの漏洩防止が課題となっている。このため、通信データに暗号化処理を行い伝送することが一般に行われるが、暗号化復号化装置による暗号化復号化は、暗号鍵と通信データを決められたアルゴリズムの演算を繰り返すことで実行されるので、演算回数を増やすことで解読難易度が向上するが、新たに処理能力が問題となる。また、マルチメディア機器の急速な普及に伴い、通信データ量が急激に増加し処理能力問題に拍車をかけているため、ほとんどの暗号化

復号化装置では、演算をハードウェアで行うことにより対応しているのが現状である。このため、暗号鍵を変更する場合ハードウェアの変更が必要となる。

【 0 0 0 3 】

このような暗号化復号化技術の一例として、特開平 5 - 1 1 0 5 5 8 号公報記載の「暗号処理装置」が知られている。

【 0 0 0 4 】

この公報では、データを暗号化し、この暗号化したデータを復号化する処理プログラムの一部又は全部を E E P R O M に格納し、暗号が解読された場合外部からの通信手段により E E P R O M のプログラムを一部又は全部を書き換える技術が記載されている。

【 0 0 0 5 】

【発明が解決しようとする課題】

上述した従来の暗号復号化装置は、アルゴリズムの演算内容が漏洩または解読された場合に通信データは簡単に復号化されてしまうこと、常に同じアルゴリズムで演算を行っているために解読法が比較的短時間で見いだされるという欠点を有している。

【 0 0 0 6 】

また、暗号解読のアルゴリズムの変更は、ハードウェアの作り直しが必要であり早急な対応ができないこと、外部からの通信手段を用いてプログラムの書き換えを行うと暗号解読プログラムデータ漏洩の危険性があるという欠点を有している。

【 0 0 0 7 】

本発明の目的は、暗号化及び復号化の処理を全てハードウェアにより高速処理し、かつ暗号解読アルゴリズムのハードウェアの変更を可能とした暗号復号化装置を提供することにある。

【 0 0 0 8 】

【課題を解決するための手段】

本発明の暗号復号化装置は、データの暗号化と暗号化データの複合化を行う暗号復号化装置において、暗号化復号化する回路を可変可能な回路装置を用い、前

記可変可能な回路装置の回路データを秘密鍵として暗号化複合化を行うことを特徴としている。

【 0 0 0 9 】

前記可変可能な回路装置の回路データを複数個有し、暗号化複合化を行うための回路データ選択情報から、前記可変可能な回路装置の回路データを選択し供給することで異なるアルゴリズムの暗号化複合化を行うことを特徴としている。

【 0 0 1 0 】

入力データを暗号化し暗号化データを出力する送信装置と、前記暗号化データを伝送するネットワーク網と、このネットワーク網を介して伝送されてきて前記暗号化データを入力し、暗号解読を行い復号化した出力データを出力する受信装置とを備え、

前記送信装置は暗号化する可変処理回路と、この可変処理回路に秘密鍵の回路データを出力するリード・オンリー・メモリ（ROM）とを有し、前記受信装置は復号化する可変処理回路と、この可変処理回路に秘密鍵の回路データを出力するリード・オンリー・メモリ（ROM）とを有していることを特徴としている。

【 0 0 1 1 】

入力データを暗号化し暗号化データを出力する送信装置と、前記暗号化データを伝送するネットワーク網と、このネットワーク網を介して伝送されてきた前記暗号化データを入力し暗号解読を行い復号化した出力データを出力する受信装置とを備え、

前記送信装置は、

前記入力データを決められた指定通りに情報を解析し、デコードして書き換え情報を出力するデータ解析部と；

暗号アルゴリズムを指定する回路データを記憶する複数のROMと；

前記書き換え情報の指示に従い前記複数のROMを選択し、選択したROMから暗号化する回路データを送出するセレクターと；

どのROMを選択するかにより暗号アルゴリズムを指定する前記回路データをもとに、自己の内部回路を書き換え、この内部回路の回路変更が完了すると終了通知信号を出力し、入力保持データを暗号化した暗号化データを前記ネットワー

ク網に送出する可変処理回路と；

前記終了通知信号を受け、それまで保持していた前記入力データを、暗号化する前記可変処理回路に前記入力保持データとして出力する暗号／復号化データ保持部と；

を有し、

前記受信装置は、

前記ネットワーク網から入力された前記暗号化データを決められた指定通りに情報を解析し、デコードして書き換え情報を出力するデータ解析部と；

暗号アルゴリズムを指定する回路データを記憶する複数のROMと；

前記書き換え情報の指示に従い前記複数のROMを選択し、選択したROMから復号化する回路データを送出するセレクターと；

どのROMを選択するかにより暗号アルゴリズムを指定する前記回路データをもとに、暗号を復号化するため自己の内部回路を書き換え、この内部回路の回路変更が完了すると終了通知信号を出力し、入力保持データの暗号化データを復号化した復号出力データを送出する可変処理回路と；

前記終了通知信号を受け、それまで保持していた前記暗号化データを、復号化する前記可変処理回路に前記入力保持データとして出力する暗号／復号化データ保持部と；

を有することを特徴としている。

【 0 0 1 2 】

入力データを暗号化し暗号化データを出力する送信装置と、前記暗号化データを伝送するネットワーク網と、このネットワーク網を介して伝送されてきた前記暗号化データを入力し暗号解読を行い復号化した出力データを出力する受信装置とを備え、

前記送信装置は、

前記入力データを決められた指定通りに情報を解析し、解析データを出力するデータ解析部と；

暗号アルゴリズムを指定する回路データを保持する複数のデータ回路部と；

前記データ解析部からの前記解析データをもとに選択信号を出力し、回路構成

を変更する第 1 の回路データを入力し、第 2 の回路データを生成出力するフィールド・プログラマブル・ゲートアレイ (Field Programmable Gate Array : 以下 F P G A と記す) 回路データ生成部と ;

前記選択信号の指示に従い、複数の回路データを選択し、選択した回路データから暗号化する前記第 1 の回路データを前記 F P G A 回路データ生成部に出力するセレクターと ;

前記 F P G A 回路データ生成部が出力する前記第 2 の回路データをもとに、自己の内部回路を書き換え、この内部回路の回路変更が完了すると終了通知信号を出力し、入力保持データを暗号化した暗号化データを前記ネットワーク網に送出する可変処理回路と ;

前記終了通知信号を受け、それまで保持していた前記入力データを新たに前記入力保持データとして前記可変処理回路に出力する暗号 / 復号化データ保持部と ;

を有し、

前記受信装置は、

前記ネットワーク網から入力された前記暗号化データを決められた指定通りに情報を解析し、解析データを出力するデータ解析部と ;

前記データ解析部からの前記解析データをもとに選択信号を出力し、回路構成を変更する第 1 の回路データを入力し、第 2 の回路データを生成出力する F P G A 回路データ生成部と ;

暗号アルゴリズムを指定する回路データを保持する複数のデータ回路部と ;

前記選択信号の指示に従い、複数の回路データを選択し、選択した回路データから暗号を復号化する前記第 1 の回路データを前記 F P G A 回路データ生成部に出力するセレクターと ;

前記 F P G A 回路データ生成部が出力する前記第 2 の回路データをもとに、暗号を復号化するため自己の内部回路を書き換え、この内部回路の回路変更が完了すると終了通知信号を出力し、入力保持データの暗号化データを復号化した復号出力データを送出する可変処理回路と ;

前記終了通知信号を受け、それまで保持していた前記入力データを新たに前記

入力保持データとして前記可変処理回路に出力する暗号／復号化データ保持部と；

を有することを特徴としている。

【 0 0 1 3 】

前記送信装置が、

前記入力データを入力保持し、終了通知信号を受けると保持していた前記入力データを保持データとして出力する暗号／復号化データ保持部と；

暗号アルゴリズムのデータを記憶するフラッシュROMと；

前記入力データを入力し、第1の回路データを前記フラッシュROMに出力し、この第1の回路データによりフラッシュROMのデータを書き換え、書き換え終了後前記フラッシュROMからの第2の回路データを入力し、自己の内部回路の変更を行い、この内部回路変更後に前記終了通知信号を前記暗号／復号化データ保持部に出力するとともに前記保持データを暗号化した出力データを出力する可変処理回路と；

を有し、

前記受信装置が、

前記暗号化した出力データを入力保持し、終了通知信号を受けると保持していた前記出力データを保持データとして出力する暗号／復号化データ保持部と；

暗号アルゴリズムのデータを記憶するフラッシュROMと；

前記暗号化した出力データを入力し、第1の回路データを前記フラッシュROMに出力し、この第1の回路データによりフラッシュROMのデータを書き換え、書き換え終了後前記フラッシュROMからの第2の回路データを入力し、自己の内部回路の変更を行い、この内部回路変更後に前記終了通知信号を前記暗号／復号化データ保持部に出力するとともに前記保持データの暗号を復号化した出力データを出力する可変処理回路と；

を有することを特徴としている。

【 0 0 1 4 】

前記送信装置が、

前記入力データを入力し、回路データを生成出力する回路データ抽出部と；

前記入力データを回路変更終了まで保持し、終了通知信号を受けると、保持していた前記入力データを保持データとして送出する暗号／復号化データ保持部と；

前記回路データにより暗号化する回路変更を行い、回路変更後前記終了通知信号を前記暗号／復号化データ保持部に出力し、変更後の回路構成によって暗号化を行った出力データを出力する可変処理回路と；

を有し、

前記受信装置が、

前記暗号化を行った出力データを入力し、回路データを生成出力する回路データ抽出部と；

前記出力データを回路変更終了まで保持し、終了通知信号を受けると、保持していた前記暗号化を行った出力データを保持データとして送出する暗号／復号化データ保持部と；

前記回路データにより復号化する回路変更を行い、回路変更後前記終了通知信号を前記暗号／復号化データ保持部に出力し、変更後の回路構成によって復号化を行った出力データを出力する可変処理回路と；

を有することを特徴としている。

【 0 0 1 5 】

前記送信装置が、

前記入力データを入力保持し、回路変更通知信号を入力すると、保持していた前記入力データを保持データとして出力する暗号／復号化データ保持部と；

暗号化コードを生成するランダム発生器と；

前記入力データが暗号化したいデータであるか復号化したいデータであるかを判定し、暗号化したいデータである場合は、前記ランダム発生器からのデータを有効にするように通知し、復号化したいデータである場合は、暗号鍵を有効にするように通知する解析データを出力するデータ解析部と；

前記解析データの通知に従い第 1 の回路データを生成出力する F P G A 回路データ生成部と；

暗号アルゴリズムを指定する回路データを記憶する複数の R O M と；

前記第 1 の回路データをもとに前記複数の ROM から回路データを取り込み、暗号アルゴリズムを指定する第 2 の回路データを出力するセレクターと；

前記第 2 の回路データを入力すると前記暗号／復号化データ保持部からの前記保持データの送出を止めるように前記回路変更通知信号を出力し、前記第 2 の回路データによって暗号化する自己の内部回路を変更し、変更が終了すると前記回路変更通知信号を停止し、再び前記保持データを送出させ、暗号化した出力データを出力する可変処理回路と；

を有し、

前記受信装置が、

前記暗号化した出力データを入力保持し、回路変更通知信号を入力すると、保持していた前記出力データを保持データとして出力する暗号／復号化データ保持部と；

暗号化コードを生成するランダム発生器と；

前記暗号化した出力データが暗号化したいデータであるか復号化したいデータであるかを判定し、暗号化したいデータである場合は、前記ランダム発生器からのデータを有効にするように通知し、復号化したいデータである場合は、暗号鍵を有効にするように通知する解析データを出力するデータ解析部と；

前記解析データの通知に従い第 1 の回路データを生成出力する F P G A 回路データ生成部と；

暗号アルゴリズムを指定する回路データを記憶する複数の ROM と；

前記第 1 の回路データをもとに前記複数の ROM から回路データを取り込み、暗号アルゴリズムを指定する第 2 の回路データを出力するセレクターと；

前記第 2 の回路データを入力すると前記暗号／復号化データ保持部からの前記保持データの送出を止めるように前記回路変更通知信号を出力し、前記第 2 の回路データによって復号化する自己の内部回路を変更し、変更が終了すると前記回路変更通知信号を停止し、再び前記保持データを送出させ、復号化した出力データを出力する可変処理回路と；

を有することを特徴としている。

【 0 0 1 6 】

前記複数のROMデータが、複数のハードウェア化されたデータ回路からのデータであり、前記セレクトーが出力する回路データを第1の回路データとして前記FPGA回路データ生成部に出力し、このFPGA回路データ生成部が出力する第2の回路データを前記可変処理回路に出力することを特徴としている。

【0017】

前記送信装置が、

前記入力データを入力保持し、回路変更通知信号を入力すると、保持していた前記入力データを保持データとして出力する暗号／復号化データ保持部と；

ある期間毎にセレクトー制御信号を生成出力するタイマーと；

暗号アルゴリズムを指定する回路データを記憶する複数のROMと；

前記セレクトー制御信号をもとに前記複数のROMを選択し暗号化する回路データを取り込み、暗号アルゴリズムを指定する回路データを出力するセレクトーと；

前記回路データを受けると前記回路変更通知信号を出力し、前記保持データの送出を停止し、前記回路データをもとに自己の内部の回路構成を変更し、変更が終了すると前記暗号／復号化データ保持部に前記保持データの送出を再開させるべく前記回路変更通知信号を停止し、前記保持データを入力し、変更した内部の回路構成によって暗号化を行い、暗号化した出力データを送出する可変処理回路と；

を有し、

前記受信装置は、

前記暗号化した出力データを入力保持し、回路変更通知信号を入力すると、保持していた前記入力データを保持データとして出力する暗号／復号化データ保持部と；

ある期間毎にセレクトー制御信号を生成出力するタイマーと；

暗号アルゴリズムを指定する回路データを記憶する複数のROMと；

前記セレクトー制御信号をもとに前記複数のROMを選択し暗号化する回路データを取り込み、暗号アルゴリズムを指定する回路データを出力するセレクトーと；

前記回路データを受けると前記回路変更通知信号を出力し、前記保持データの送出を停止し、前記回路データをもとに自己の内部の回路構成を変更し、変更が終了すると前記暗号／復号化データ保持部に前記保持データの送出を再開させるべく前記回路変更通知信号を停止し、前記保持データを入力し、変更した内部の回路構成によって復号化を行い、復号化した出力データを送出する可変処理回路と；

を有することを特徴としている。

【0018】

前記複数のROMデータが、複数のハードウェア化されたデータ回路部からのデータであり、前記ランダム発生器が、ある期間毎にセレクター制御信号を生成出力するタイマーであり、前記セレクターが出力する回路データを第1の回路データとして前記FPGA回路データ生成部に出力し、このFPGA回路データ生成部が出力する第2の回路データを前記可変処理回路に出力することを特徴としている。

【0019】

また、前記可変処理回路が、フィールド・プログラマブル・ゲートアレイ（FPGA）であることを特徴としている。

【0020】

【発明の実施の形態】

次に、本発明の実施の形態について図面を参照して説明する。

【0021】

図1は本発明の暗号復号化装置の一つの実施の形態を示すブロック図である。

【0022】

図1に示す本実施の形態は、入力データ101を暗号化し暗号化データ110を出力する送信装置102と、暗号化データ110を伝送するネットワーク網111と、このネットワーク網111を介して伝送されてきて暗号化データ113を入力し、暗号解読を行い復号化した出力データ112を出力する受信装置106とから構成されている。

【0023】

なお、送信装置 1 0 2 は暗号化する可変処理回路 1 0 3 と、この可変処理回路 1 0 3 に秘密鍵の回路データ 1 0 5 を出力するリード・オンリー・メモリである ROM 1 0 4 とを有し、受信装置 1 0 6 は復号化する可変処理回路 1 0 7 と、この可変処理回路 1 0 7 に秘密鍵の回路データ 1 0 9 を出力するリード・オンリー・メモリである ROM 1 0 8 とを有している。

【 0 0 2 4 】

なお、上述の可変処理回路 1 0 3, 1 0 7 は具体的な回路素子として F P G A (F i e l d P r o g r a m a b l e G a t e A r r a y) が使用され、任意の回路構成がプログラムデータの変更により容易に実現できる。

【 0 0 2 5 】

次に動作を説明する。

【 0 0 2 6 】

入力データ 1 0 1 は可変処理回路 1 0 3 により暗号化され、この暗号化された暗号化データ 1 1 0 は一般的なネットワーク網 1 1 1 に供給される。受信装置 1 0 6 はネットワーク網 1 1 1 から暗号化データ 1 1 3 を入力する。暗号化データ 1 1 3 は、復号化のため可変処理回路 1 0 7 で復号化処理がなされ、出力データ 1 1 2 として出力される。

【 0 0 2 7 】

なお、ROM 1 0 4 は秘密鍵を変更する場合に取り替えて、可変処理回路 1 0 3 の書き換えを行う。取り替えられた ROM 1 0 4 から新しい暗号化アルゴリズムを生成する回路データ 1 0 5 が可変処理回路 1 0 3 に出力され、可変処理回路 1 0 3 の回路構成を変更することにより、入力データ 1 0 1 は新しい形式の暗号化データ 1 1 0 が出力される。新しい形式の暗号化データ 1 1 0 に対し、受信装置 1 0 6 の可変処理回路 1 0 7 も新しい ROM 1 0 8 を用いて回路構成を変更し、新しい形式の暗号化データ 1 1 3 の復号化を行う。

【 0 0 2 8 】

つまり、可変処理回路 1 0 3, 1 0 7 の回路変更は取り替え可能な ROM 1 0 4, 1 0 8 が出力する回路データ 1 0 5, 1 0 9 により行われる。

【 0 0 2 9 】

上述の通り、送信装置 1 0 2 には、暗号化する可変処理回路 1 0 3 と回路データ 1 0 5 が記憶されている ROM 1 0 4 とを有しており、送信装置 1 0 2 を起動させたとき、ROM 1 0 4 から回路データ 1 0 5 が暗号化する可変処理回路 1 0 3 へ送出される。回路データ 1 0 5 によって暗号化する可変処理回路 1 0 3 の回路構成が新しく形成され、入力データ 1 0 1 を順次暗号化する可変処理回路 1 0 3 となる。この暗号化する可変処理回路 1 0 3 によって暗号化された暗号化データ 1 1 0 は、ネットワーク網 1 1 1 に送出される。

【 0 0 3 0 】

受信装置 1 0 6 も同様に復号化する可変処理回路 1 0 7 と回路データ 1 0 9 が記憶されている ROM 1 0 8 とを有しており、受信装置 1 0 6 を起動させたとき、ROM 1 0 8 から回路データ 1 0 9 が復号化する可変処理回路 1 0 7 へ送出される。回路データ 1 0 9 によって復号化する可変処理回路 1 0 7 の回路構成が新しく形成され、暗号化データ 1 1 3 を順次復号化する可変処理回路 1 0 7 となる。この可変処理回路 1 0 7 により、ネットワーク網 1 1 1 から受信した暗号化データ 1 1 3 を復号化し、出力データ 1 1 2 を生成出力する。

【 0 0 3 1 】

ROM 1 0 4, ROM 1 0 8 は、秘密鍵を変更する場合に取り替えて、暗号化する可変処理回路 1 0 3、復号化する可変処理回路 1 0 7 の書き換えデータを各々生成する。こうして生成された回路データ 1 0 5, 1 0 9 は暗号化する可変処理回路 1 0 3、復号化する可変処理回路 1 0 7 に出力され、回路構成を変更することにより新しい形式の暗号化および復号化に対応することになる。

【 0 0 3 2 】

図 2 は本発明の暗号復号化装置の一例を示す詳細ブロック図である。

【 0 0 3 3 】

なお、図 2 において図 1 に示す構成要素に対応するものは同一の参照数字または符号を付し、その説明を省略する。

【 0 0 3 4 】

図 2 を参照すると、入力データ 2 0 2 を暗号化し暗号化データ 2 1 1 を出力する送信装置 2 0 1 と、暗号化データ 2 1 1 を伝送するネットワーク網 1 1 1 と、

このネットワーク網 111 を介して伝送されてきて暗号化データ 213 を入力し、暗号解読を行い復号化した出力データ 214 を出力する受信装置 201a とから構成されている。

【0035】

なお、送信装置 201 に入力する入力データ 202 は、決められた指定に従い書き換え情報が付随した信号である。

【0036】

入力データ 202 は、データ解析部 203 と暗号／復号化データ保持部 204 に出力される。データ解析部 203 では、決められた指定通りに情報を解析し、デコードして書き換え情報 216 をセレクター 205 に出力する。セレクター 205 は、書き換え情報 216 の指示に従い ROM 206, 206a, 206b, 206n を選択し、暗号化する可変処理回路 207 に回路データ 208 を送出する。暗号化する可変処理回路 207 では、回路データ 208 をもとにして、暗号化する可変処理回路 207 の内部回路を書き換え、どの ROM を選択するかにより暗号アルゴリズムを選択することができる。暗号化する可変処理回路 207 で回路変更が完了すると、可変処理回路 207 は終了通知信号 209 を暗号／復号化データ保持部 204 に出力する。終了通知信号 209 を受けた暗号／復号化データ保持部 204 は、それまで保持していた入力データ 202 を暗号化する可変処理回路 207 に入力保持データ 210 として出力する。こうして、可変処理回路 207 は入力データ 202 の暗号化を行い、暗号化データ 211 をネットワーク網 111 に送出する。

【0037】

ネットワーク網 111 から入力された暗号化データ 213 は、データ解析部 203a と暗号／復号化データ保持部 204a に送出される。データ解析部 203a では、決められた指定通りに情報を解析し、デコードして書き換え情報 216a をセレクター 205a に出力する。セレクター 205a は、書き換え情報 216a の指示に従い ROM 215, 215a, 215b, 215n を選択し、復号化する可変処理回路 207a に回路データ 208a を出力する。復号化する可変処理回路 207a では、回路データ 208a をもとに暗号を復号化する可変処理

回路 2 0 7 a の内部回路を書き換える。復号化する可変処理回路 2 0 7 a で回路変更が完了すると、終了通知信号 2 0 9 a を暗号／復号化データ保持部 2 0 4 a に出力する。終了通知信号 2 0 9 a を受けた暗号／復号化データ保持部 2 0 4 a は、それまで保持していた暗号化データ 2 1 3 を復号化する可変処理回路 2 0 7 a に入力保持データ 2 1 0 a として出力する。かくして、可変処理回路 2 0 7 a は暗号化データ 2 1 3 の復号化を行い出力データ 2 1 4 を出力する。

【 0 0 3 8 】

図 3 は図 2 の動作を示すタイムチャートである。

【 0 0 3 9 】

次に、図 2 および図 3 を参照して本実施の形態の動作をより詳細に説明する。

【 0 0 4 0 】

入力データ 2 0 2 はヘッダ情報と暗号化するデータ信号とからなり、データ解析部 2 0 3 は入力データ 2 0 2 から書き換え情報 2 1 6 を抽出すると、書き換え情報 2 1 6 のデータをデコードしてセレクター 2 0 5 を制御する。

【 0 0 4 1 】

これによって、ROM 2 0 6, 2 0 6 a, 2 0 6 b, 2 0 6 n のデータを切り替え、回路データ 2 0 8 を生成する。ROM のデータを切り換えると同時に可変処理回路 2 0 7 に書き換え信号を生成し、暗号化する可変処理回路 2 0 7 は可変処理回路 2 0 7 の書き換え信号の立ち上がりで初期化する。暗号化する可変処理回路 2 0 7 は回路データ 2 0 8 をもとに回路を変更し、変更が終わると終了通知信号 2 0 9 を出力する。終了通知信号 2 0 9 を受けるまで暗号／復号化データ保持部 2 0 4 では入力データ 2 0 2 を保持し、この保持していた保持データ 2 1 0 を入力された順に暗号化する可変処理回路 2 0 7 に送出する。暗号化する可変処理回路 2 0 7 により保持データ 2 1 0 の暗号化の処理を行い暗号化データ 2 1 1 を生成出力する。

【 0 0 4 2 】

図 4 は図 2 の全体動作を示すフローチャートである。

【 0 0 4 3 】

入力データ 2 0 2 を受けると暗号／復号化動作を行う（ステップ 1 : S 1 ）。

【0044】

ステップ2 (S2) で書き換え情報216, 216a受信の判定を行い、書き換え情報216, 216aを受信するまではステップ1に戻り、暗号／復号化動作を繰り返す。ステップ2で書き換え情報を受信すると、受信した書き換え情報216, 216aに対してデコードする(ステップ3:S3)。

【0045】

次にセレクター205, 205aの制御を行い、暗号／復号化する可変処理回路207, 207aに書き換え信号を送出し、また暗号／復号化データ保持部204, 204aにデータの保持を開始させる(ステップ4:S4)。その後、セレクター205, 205aによって選択された回路データを暗号／復号化する可変処理回路207, 207aに送出する(ステップ5:S5)。次のステップ6 (S6) で暗号／復号化する可変処理回路207, 207aの書き換えが完了したかの判断を行い、完了していない場合ステップ1 (S1) に戻り、完了している場合ステップ7 (S7) に進み終了通知信号209, 209aを生成し、暗号／復号化する可変処理回路207, 207aの書き換え信号をリセットする。また、暗号／復号化データ保持部204, 204aで保持していた信号を暗号／復号化する可変処理回路207, 207aにデータを送出開始する(ステップ8:S8)。

【0046】

上述の通り、回路データ208, 208aを秘密鍵としているので、回路データをもった送受信機のみ解読可能な暗号通信が可能となる。従ってセキュリティの向上を図ることができる。さらに、複数のROMデータが設けられているので、通信毎に暗号鍵を変更できることになる。この結果、一つのデータを複数の回路構成によって暗号化することができる。秘密鍵が回路データとなっているので、万一秘密鍵が漏れても同様の回路構成を作る事が困難であるため、より高度な暗号回路が構成できることになる。

【0047】

図5は本発明の暗号復号化装置の第2の実施の形態を示す詳細ブロック図である。

【 0 0 4 8 】

なお、図 5 において図 2 に示す構成要素に対応するものは同一の参照数字または符号を付し、その説明を省略する。

【 0 0 4 9 】

図 5 を参照すると、入力データ 3 0 3 を暗号化し暗号化データ 3 1 4 を出力する送信装置 3 0 2 と、暗号化データ 3 1 4 を伝送するネットワーク網 1 1 1 と、このネットワーク網 1 1 1 を介して伝送されてきて暗号化データ 3 1 5 を入力し、暗号解読を行い復号化した出力データ 3 1 6 を出力する受信装置 3 0 2 a とから構成されている。

【 0 0 5 0 】

送信装置 3 0 2 に入力する入力データ 3 0 3 は、決められた指定に従い書き換え情報が付随した送受信信号である。入力データ 3 0 3 は、データ解析部 3 0 4 と暗号／復号化データ保持部 3 0 5 に送出される。データ解析部 3 0 4 では、決められた指定通りに情報を解析し、解析データ 3 1 7 を F P G A 回路データ生成部 3 0 6 に送出する。F P G A は既述の通り、F i e l d P r o g r a m a b l e G a t e A r r a y の素子で、F P G A 回路データ生成部 3 0 6 は可変処理回路 3 0 1 の回路構成を変更する回路データを生成する。

【 0 0 5 1 】

F P G A 回路データ生成部 3 0 6 では、データ解析部 3 0 4 からの解析データ 3 1 7 をもとに選択信号 3 0 8 をセレクター 3 0 9 に出力し、データ回路部 3 0 7, 3 0 7 a, 3 0 7 b, 3 0 7 n を選択する。選択信号 3 0 8 により、書き換え情報の要求通りに組み合わせた回路データ 3 1 0 を F P G A 回路データ生成部 3 0 6 に出力する。

【 0 0 5 2 】

暗号化する可変処理回路 3 0 1 では、F P G A 回路データ生成部 3 0 6 が出力する回路データ 3 1 1 をもとに回路を変更する。可変処理回路 3 0 1 で回路変更が終了すると、終了通知信号 3 1 2 を暗号／復号化データ保持部 3 0 5 に出力する。終了通知信号 3 1 2 を受けた暗号／復号化データ保持部 3 0 5 は、入力データ 3 0 3 を新たに入力保持データ 3 1 3 として頭から可変処理回路 3 0 1 に送出

する。入力保持データ 3 1 3 を受信した可変処理回路 3 0 1 は、書き換えた回路によって暗号化を行う。こうして、可変処理回路 3 0 1 は暗号化を行い暗号化データ 3 1 4 をネットワーク網 1 1 1 に送出する。

【 0 0 5 3 】

ネットワーク網 1 1 1 から入力された暗号化データ 3 1 5 は、データ解析部 3 0 4 a と暗号／復号化データ保持部 3 0 5 a に送出される。データ解析部 3 0 4 a では、決められた指定通りに情報を解析し、解析データ 3 1 7 a を F P G A 回路データ生成部 3 0 6 a に送出する。F P G A 回路データ生成部 3 0 6 a では、データ解析部 3 0 4 a からの解析データ 3 1 7 a をもとに選択信号 3 0 8 a をセレクター 3 0 9 a に送り、データ回路部 3 1 6, 3 1 6 a, 3 1 6 b, 3 1 6 n を選択する。選択信号 3 0 8 a により、書き換え情報の要求通りに組み合わせた回路データ 3 1 0 a を F P G A 回路データ生成部 3 0 6 a に出力する。復号化する可変処理回路 3 0 1 a では、F P G A 回路データ生成部 3 0 6 a が出力する回路データ 3 1 1 a をもとに回路を変更する。可変処理回路 3 0 1 a で回路変更が終了すると、終了通知信号 3 1 2 a を暗号／復号化データ保持部 3 0 5 a に出力する。終了通知信号 3 1 2 a を受けた暗号／復号化データ保持部 3 0 5 a は、入力データ 3 0 3 a を新たに入力保持データ 3 1 3 a として頭から可変処理回路 3 0 1 a に送出する。入力保持データ 3 1 3 a を受信した可変処理回路 3 0 1 a は、書き換えた回路によって復号化を行う。かくして、可変処理回路 3 0 1 a は復号化を行い出力データ 3 1 6 を出力する。

【 0 0 5 4 】

上述の通り本第 2 の実施の形態は R O M 回路からの R O M データとは異なり、複数個用意されたデータ回路部 3 0 7, 3 0 7 a, 3 0 7 b, 3 0 7 n を書き換え情報に従って組み合わせ、一つの回路構成を形成するようにしたものである。

【 0 0 5 5 】

送信装置 3 0 2 に入力する入力データ 3 0 3 は、決められた指定に従い書き換え情報を付随した信号であり、入力データ 3 0 3 は、データ解析部 3 0 4 と暗号／復号化データ保持部 3 0 5 に送出される。データ解析部 3 0 4 では、決められた指定通りに情報を解析し、解析データ 3 1 7 を F P G A 回路データ生成部 3 0

6に送出する。FPGA回路データ生成部306では、データ解析部304からの解析データ317をもとにデータ回路部307、307a、307b、307nを任意に選択する。選択信号308をセレクター309に送り、回路データ310を書き換え情報の要求通りに組み合わせて、可変処理回路301のデータの生成を行う。暗号化する可変処理回路301では、その組み合わせて作り出された回路データ311をもとに回路を変更する。暗号化する可変処理回路301で回路変更が終了すると、終了通知信号312を暗号／復号化データ保持部305に出力する。終了通知信号312を受けた暗号／復号化データ保持部305は、入力データ303を暗号化する可変処理回路301に頭から送出する。入力保持データ313を受信した暗号化する可変処理回路301は、書き換えた回路によって暗号復号化を行う。これにより、データの数の組み合わせ分だけの暗号復号化の回路構成を生成できる。

【0056】

図6は本発明の暗号復号化装置の第3の実施の形態を示すブロック図である。

【0057】

なお、ここでは暗号化を行う送信装置と暗号の復号化を行う受信装置とを、ネットワーク網111を介して分離した表示にせずに、一つのブロックとして暗号／復号化として一括表示にして説明の簡略化を図る。送信装置は暗号化、受信装置は復号化として暗号／復号化を読み替えるものとする。

【0058】

図6を参照すると、暗号復号化装置401に入力する入力データ402を暗号／復号化する可変処理回路403に入力し、同時に暗号／復号化データ保持部404に保持しておく。暗号／復号化する可変処理回路403によって、回路データ405を抽出し、FLASH ROM406を書き換える。FLASH ROM406の書き換えが終了したら、暗号／復号化する可変処理回路403をリセットしFLASH ROM406に書き込まれた回路データ407を読み出し可変処理回路403の内部回路を変更する。暗号／復号化する可変処理回路403の内部回路が生成完了したら、暗号／復号化データ保持部404に終了通知信号408を送出する。暗号／復号化データ保持回路404で保持しておいた保持デ

ータ 4 0 9 を暗号／復号化する可変処理回路 4 0 3 を通して、暗号復号化を行った出力データ 4 1 0 を送出する。

【 0 0 5 9 】

このように、本形態では多数の暗号アルゴリズムを決定する回路データにより変更できることになる。

【 0 0 6 0 】

図 7 は本発明の暗号復号化装置の第 4 の実施の形態を示すブロック図である。

【 0 0 6 1 】

なお、ここでは暗号化を行う送信装置と暗号の復号化を行う受信装置とを、ネットワーク網 1 1 1 を介して分離した表示にせずに、一つのブロックとして暗号／復号化として一括表示にして説明の簡略化を図る。送信装置は暗号化、受信装置は復号化として暗号／復号化を読み替えるものとする。

【 0 0 6 2 】

図 7 を参照すると、暗号復号化装置 5 0 1 に入力する入力データ 5 0 2 を、回路データ抽出部 5 0 3 で予め定めておいたフォーマットに従って抽出し、回路データ 5 0 4 を生成する。この回路データ 5 0 4 により、暗号／復号化する可変処理回路 5 0 5 の回路変更を行う。入力データ 5 0 2 は、暗号／復号化データ保持部 5 0 6 に回路変更終了まで保持しておき、暗号／復号化データ保持部 5 0 6 が終了通知信号 5 0 7 を受けると、暗号／復号化する可変処理回路 5 0 5 へ保持していた保持データ 5 0 9 を送出し、暗号／復号化する可変処理回路 5 0 5 の新しい回路構成によって暗号復号化を行い出力データ 5 0 8 を出力する。

【 0 0 6 3 】

図 8 は本発明の暗号復号化装置の第 5 の実施の形態を示すブロック図である。

【 0 0 6 4 】

なお、ここでは暗号化を行う送信装置と暗号の復号化を行う受信装置とを、ネットワーク網 1 1 1 を介して分離した表示にせずに、一つのブロックとして暗号／復号化として一括表示にして説明の簡略化を図る。送信装置は暗号化、受信装置は復号化として暗号／復号化を読み替えるものとする。

【 0 0 6 5 】

図 8 を参照すると、暗号復号化装置 6 0 1 に入力する入力データ 6 0 2 は、暗号／復号化データ保持部 6 0 3 に一度保持される。データ解析部 6 0 4 では、入力された入力データ 6 0 2 が暗号化したいデータであるか復号化したいデータであるかを判定する。データ解析部 6 0 4 は暗号化したいデータである場合は、ランダム発生器 6 0 6 からのデータを有効にするように F P G A 回路データ生成部 6 0 5 に通知し、復号化したいデータである場合は、データ解析部 6 0 4 で抽出した暗号鍵を有効にするように F P G A 回路データ生成部 6 0 5 に通知すると共に抽出した暗号鍵を送出する。F P G A 回路データ生成部 6 0 5 では、データ解析部 6 0 4 からの解析データ 6 1 4 の通知に従い可変処理回路 6 1 0 のための回路データ 6 1 5 を生成する。ランダム発生器 6 0 6 からの信号を有効にして可変処理回路 6 1 0 の回路データ 6 0 9 を生成する場合は、ランダム発生器 6 0 6 からの信号を取り込み、そのデータをもとにセレクター 6 0 7 を制御し、R O M 6 0 8, 6 0 8 a, 6 0 8 b, 6 0 8 n から回路データを取り込み、回路データを組み合わせて回路データ 6 0 9 を生成する。回路データ 6 0 9 を受信した可変処理回路 6 1 0 は、暗号／復号化データ保持部 6 0 3 からの保持データ 6 1 1 の送出手を止めるように回路変更通知信号 6 1 2 を出力し、回路データ 6 0 9 によって暗号／復号化する可変処理回路 6 1 0 の内部の構成を変更する。変更が終了すると回路変更通知信号 6 1 2 を停止し、再び暗号／復号化データ保持部 6 0 3 からの保持データ 6 1 1 を送出手してもらう。新しい回路構成となった暗号／復号化する可変処理回路 6 1 0 は暗号復号化を行い、出力データ 6 1 3 を送出手する。

【 0 0 6 6 】

上述の通り、書き換え情報の生成をランダム発生器 6 0 6 に任せることでシステムへの負荷の軽減を図ったものである。

【 0 0 6 7 】

図 9 は本発明の暗号復号化装置の第 6 の実施の形態を示すブロック図である。

【 0 0 6 8 】

なお、ここでは暗号化を行う送信装置と暗号の復号化を行う受信装置とを、ネットワーク網 1 1 1 を介して分離した表示にせずに、一つのブロックとして暗号／復号化として一括表示にして説明の簡略化を図る。送信装置は暗号化、受信装

置は復号化として暗号／復号化を読み替えるものとする。

【0069】

図9を参照すると、暗号復号化装置701に入力する入力データ702は、暗号／復号化データ保持部703に一旦収納される。データ解析部704では、入力された入力データ702が暗号化したいデータであるか復号化したいデータであるかを判定する。暗号化したいデータである場合は、ランダム発生器706からのデータを有効にするようにFPGA回路データ生成部705に通知し、復号化したいデータである場合は、データ解析部704で抽出した暗号鍵を有効にするようにFPGA回路データ生成部705に通知すると共に抽出した暗号鍵を送出する。FPGA回路データ生成部705では、データ解析部704からの解析データ714の通知に従いFPGAの回路データを生成する。ランダム発生器706からの信号を有効にしてFPGAの回路データを生成する場合は、ランダム発生器706からの信号を取り込み、そのデータをもとにセレクター707を制御し、データ回路部708、708a、708b、708nから回路データ715を取り込み、回路データ715を組み合わせる回路データ709を生成する。回路データ709を受信した可変処理回路710は、暗号／復号化データ保持部703からの保持データ711の送出を止めるように回路変更通知信号712によって連絡し、FPGA用回路データ709によって暗号／復号化する可変処理回路710の内部の構成を変更する。変更が終了すると回路変更通知信号712を停止し、再び暗号／復号化データ保持部703からの保持データ711を送出してもらい、新しい回路構成となった暗号／復号化する可変処理回路710は暗号復号化を行い、出力データ713を送出する。これにより、よりハードウェア化されるため、システムでの負荷を最小限に抑えられると同時により多くの暗号鍵を備えることになる。

【0070】

図10は本発明の暗号復号化装置の第7の実施の形態を示すブロック図である。

【0071】

なお、ここでは暗号化を行う送信装置と暗号の復号化を行う受信装置とを、ネ

ットワーク網 1 1 1 を介して分離した表示にせずに、一つのブロックとして暗号／復号化として一括表示にして説明の簡略化を図る。送信装置は暗号化、受信装置は復号化として暗号／復号化を読み替えるものとする。

【 0 0 7 2 】

図 1 0 を参照すると、暗号復号化装置 8 0 1 に入力する入力データ 8 0 2 は、暗号／復号化データ保持部 8 0 3 に一度保持される。暗号／復号化データ保持部 8 0 3 では、暗号／復号化する可変処理回路 8 0 4 からの回路変更通知信号 8 0 5 によって出力を停止されている場合を除いて、常に暗号／復号化する可変処理回路 8 0 4 へ保持データ 8 0 6 を送出する。暗号／復号化する可変処理回路 8 0 4 では、暗号／復号化データ保持部 8 0 3 からの保持データ 8 0 6 を内部の回路構成によって暗号復号化を行い出力データ 8 0 7 を送出する。タイマー 8 0 8 は、ある期間毎にセレクター 8 0 9 を制御するセレクター制御信号 8 1 2 を生成する。セレクター 8 0 9 では、タイマー 8 0 8 からのセレクター制御信号 8 1 2 をもとに ROM 8 1 0, 8 1 0 a, 8 1 0 b, 8 1 0 n を選択し、暗号／復号化する可変処理回路 8 0 4 に回路データ 8 1 1 を送出する。回路データ 8 1 1 を受けた暗号／復号化する可変処理回路 8 0 4 は、一旦出力データ 8 0 7 の生成を止め、回路変更通知信号 8 0 5 を暗号／復号化データ保持部 8 0 3 に送り、保持データ 8 0 6 の送出を停止させる。暗号／復号化する可変処理回路 8 0 4 は、回路データ 8 1 1 をもとに内部の回路構成を変更し、変更が終了すると暗号／復号化データ保持部 8 0 3 に保持データ 8 0 6 の送出を再開させるべく、回路変更通知信号 8 0 5 を止めて保持データ 8 0 6 を入力する。暗号／復号化する可変処理回路 8 0 4 は、変更した内部の回路構成によって暗号復号化を行い、出力データ 8 0 7 を送出する。これにより、暗号解読のキーワードを全く送出しなくなるため、第三者による暗号解読がより困難になる。

【 0 0 7 3 】

送受信側に同期を取ったタイマーを備えることでより機密性の高いを構成としている。

【 0 0 7 4 】

図 1 1 は本発明の暗号復号化装置の第 8 の実施の形態を示すブロック図である

【 0 0 7 5 】

なお、ここでは暗号化を行う送信装置と暗号の復号化を行う受信装置とを、ネットワーク網 1 1 1 を介して分離した表示にせず、一つのブロックとして暗号／復号化として一括表示にして説明の簡略化を図る。送信装置は暗号化、受信装置は復号化として暗号／復号化を読み替えるものとする。

【 0 0 7 6 】

図 1 1 を参照すると、暗号復号化装置 9 0 1 に入力する入力データ 9 0 2 は、暗号／復号化データ保持部 9 0 3 に一度保持される。暗号／復号化データ保持部 9 0 3 では、暗号／復号化する可変処理回路 9 0 4 からの回路変更通知信号 9 0 5 によって出力を停止されている場合を除いて、常に暗号／復号化する可変処理回路 9 0 4 へ保持データ 9 0 6 を送出する。暗号／復号化する可変処理回路 9 0 4 では、暗号／復号化データ保持部 9 0 3 からの保持データ 9 0 6 を内部の回路構成によって暗号復号化を行い出力データ 9 0 7 を送出する。

【 0 0 7 7 】

タイマー 9 0 8 は、ある期間毎に F P G A 回路データ生成部 9 0 9 に信号を送出する。F P G A 回路データ生成部 9 0 9 では、タイマー 9 0 8 から受けた信号情報をもとに、セレクター 9 1 0 を制御し、選択されたデータ回路部 9 1 1, 9 1 1 a, 9 1 1 b, 9 1 1 n を取り込み、取り込んだ回路データ 9 1 2 を組み合わせ可変処理回路 9 0 4 の回路データ 9 1 3 を生成し、生成した回路データ 9 1 3 を暗号／復号化する可変処理回路 9 0 4 に送出する。回路データ 9 1 3 を入力した暗号／復号化する可変処理回路 9 0 4 は、一度出力データ 9 0 7 の生成を止め、回路変更通知信号 9 0 5 を暗号／復号化データ保持部 9 0 3 に送り、出力データ 9 0 7 の送出を停止させ、暗号／復号化する可変処理回路 9 0 4 は、回路データ 9 1 3 をもとに内部の回路構成を変更し、変更が終了すると暗号／復号化データ保持部 9 0 3 に保持データ 9 0 6 の送出を再開させる。回路変更通知信号 9 0 5 を止めて、保持データ 9 0 6 を入力する。暗号／復号化する可変処理回路 9 0 4 は、変更した内部の回路構成によって暗号復号化を行い、出力データ 9 0 7 を送出する。これにより、より機密性の高く、より柔軟性のある回路構成となる

ため、第三者による暗号解読は困難になる。

【0078】

図12は本発明の暗号復号化装置を利用したシステムブロック図である。

【0079】

図12を参照すると、親局1の秘密鍵管理部2から、定期的に暗号／復号化するFPGA変更用のデータを子局3，4へ送出する。子局3，4側では、前回までの回路データを元にした可変処理回路5，6によって、回路データ7，8を認識し、FLASH ROM9，10に書き込む。親局1側で更新通知を子局3，4全てに送出し、その通知が来るとFLASH ROM9，10に蓄えてあった回路データ7，8をもとに、子局3，4が一斉に暗号／復号化する可変処理回路5，6の回路構成を変更する。暗号／復号化する可変処理回路5，6は新しい秘密鍵によって通信の運用を行えるようになる。回路データ7，8は、通常の通信中に少しずつ送出しておくとともに、通常はダミービット扱いの信号としてFLASH ROM9，10内部を徐々に変更しておく。

【0080】

図13は可変処理回路による暗号復号化装置の一例を示すブロック図である。

【0081】

図13を参照にすると、暗号復号化装置11は、入力データ12を回路データ抽出部13、回路データ保持部14、暗号／復号化部15の全てに入力されている。回路データ抽出部13では、入力データ12を保持し、内部情報を解析し回路データ17を抽出する。抽出した回路データ17を、回路データ保持部14が保持しておき、回路データ18として暗号／復号化部15に送出する。暗号／復号化部15では、回路データ保持部14からの回路データ18をもとに内部回路構成を変更する。変更が終了すると、回路データ抽出部13で蓄えていた入力データ12の暗号復号化の処理を行い、出力データ16を生成出力する。

【0082】

なお、FLASH ROMを用いているが、この部分に可変処理回路を並べるという技術思想を用いても得られる。

【0083】

つまり本装置のFLASH ROM部にFPGAとしての可変処理回路を用い、また回路構成抽出部自身にもFPGAを使用している。従って、各FPGAの回路構成を全て解読できなければ第三者が解読できないという作用が得られる。図13において、暗号復号化装置11は、3つのFPGAとして回路データ抽出部13、回路データ保持部14、暗号／復号化部15を持つ。入力される入力データ12は、回路データ抽出部13、回路データ保持部14、暗号／復号化部15の全てのFPGAに入力される。回路データ抽出部13では、回路情報の抽出を行う。回路データ保持部14では、抽出した回路データ17を保持しておく。暗号／復号化部15では、回路データ保持部14からの回路データ18によって回路構成を変更する。

【0084】

変更が完了すると、回路データ抽出部13へ終了通知信号19を出力する。終了通知信号19を受信した回路データ抽出部13は、保持していた保持データ20を暗号／復号化部15に送出する。暗号／復号化部15では、新しい回路構成で暗号復号化し、データを送出する。これにより、暗号解読のためには、様々な要素を持つことになる。

【0085】

本形態では、相互に回路データ抽出部を備えているので、一つのFPGAの回路変更がうまくいかなかった、あるいは、故障してしまっても他のFPGAで書き換えを可能にするという相乗的な効果を奏する。

【0086】

本実施例のFPGAはFPGA搭載の特定用途向け集積回路であるASIC (Application Specific Integrated Circuit) に変更してもよい。さらに、複雑な回路構成をASICで実現できれば、より気密性の高いデータ転送に有効である。

【0087】

【発明の効果】

以上説明したように、本発明の暗号復号化装置は、可変処理回路の回路データが可変できるので、処理能力を落とすことなく暗号アルゴリズムの演算を変更す

ることができるという効果を有している。

【 0 0 8 8 】

また、可変処理回路の回路データの変換アルゴリズムを非公開とすることでより難解な解読度が実現可能となり、暗号解読プログラムデータの漏洩を防ぐことができるという効果を有している。

【図面の簡単な説明】

【図 1】

本発明の暗号復号化装置の一つの実施の形態を示すブロック図である。

【図 2】

本発明の暗号復号化装置の一例を示す詳細ブロック図である。

【図 3】

図 2 の動作を示すタイムチャートである。

【図 4】

図 2 の全体動作を示すフローチャートである。

【図 5】

本発明の暗号復号化装置の第 2 の実施の形態を示す詳細ブロック図である。

【図 6】

本発明の暗号復号化装置の第 3 の実施の形態を示すブロック図である。

【図 7】

本発明の暗号復号化装置の第 4 の実施の形態を示すブロック図である。

【図 8】

本発明の暗号復号化装置の第 5 の実施の形態を示すブロック図である。

【図 9】

本発明の暗号復号化装置の第 6 の実施の形態を示すブロック図である。

【図 1 0】

本発明の暗号復号化装置の第 7 の実施の形態を示すブロック図である。

【図 1 1】

本発明の暗号復号化装置の第 8 の実施の形態を示すブロック図である。

【図 1 2】

本発明の暗号復号化装置を利用したシステムブロック図である。

【図 1 3】

可変処理回路による暗号復号化装置の一例を示すブロック図である。

【符号の説明】

- 1 親局
- 2 秘密鍵管理部
- 3, 4 子局
- 5, 6 可変処理回路
- 7, 8 回路データ
- 9, 10 FLASH ROM
- 11 暗号復号化装置
- 12 入力データ
- 13 回路データ抽出部
- 14 回路データ保持部
- 15 暗号／復号化部
- 16 出力データ
- 17, 18 回路データ
- 19 終了通知信号
- 20 保持データ
- 101 入力データ
- 102 送信装置
- 103, 107 可変処理回路
- 104, 108 ROM
- 105, 109 回路データ
- 106 受信装置
- 110 暗号化データ
- 111 ネットワーク網
- 112 出力データ
- 113 暗号化データ

- 201 送信装置
- 201a 受信装置
- 202 入力データ
- 203, 203a データ解析部
- 204, 204a 暗号／復号化データ保持部
- 205, 205a セレクター
- 206, 206a, 206b, 206n ROM
- 207, 207a 可変処理回路
- 208, 208a 回路データ
- 209, 209a 終了通知信号
- 210, 210a 入力保持データ
- 211 暗号化データ
- 213 暗号化データ
- 214 出力データ
- 215, 215a, 215b, 215n ROM
- 216, 216a 書き換え情報
- 301, 301a 可変処理回路
- 302 送信装置
- 302a 受信装置
- 303 入力データ
- 304, 304a データ解析部
- 305, 305a 暗号／復号化データ保持部
- 306, 306a FPGA回路データ生成部
- 307, 307a, 307b, 307n データ回路部
- 308, 308a 選択信号
- 309, 309a セレクター
- 310, 310a 回路データ
- 311, 311a 回路データ
- 312, 312a 終了通知信号

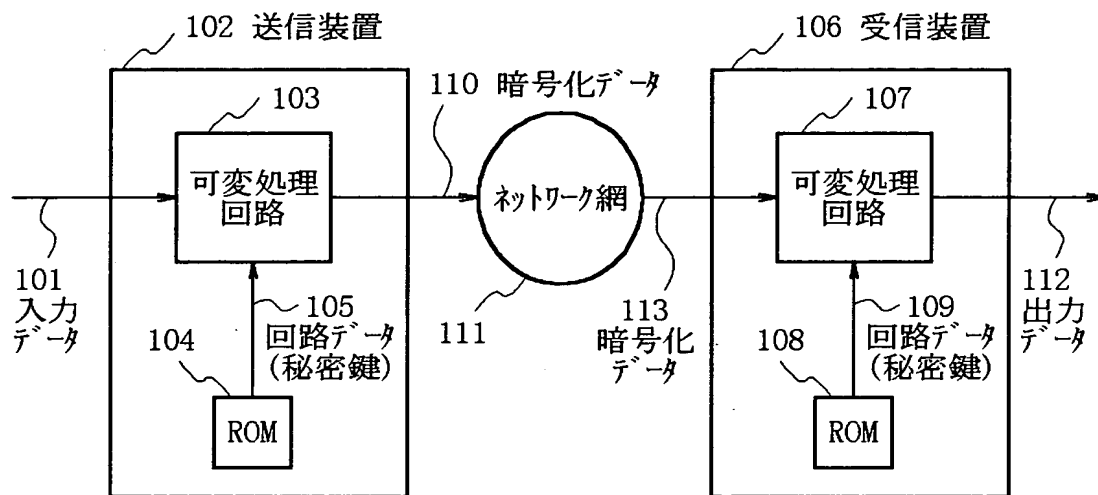
3 1 3, 3 1 3 a 入力保持データ
 3 1 4, 3 1 5 暗号化データ
 3 1 6, 3 1 6 a, 3 1 6 b, 3 1 6 n データ回路部
 3 1 7, 3 1 7 a 解析データ
 4 0 1 暗号復号化装置
 4 0 2 入力データ
 4 0 3 可変処理回路
 4 0 4 暗号／復号化データ保持部
 4 0 5 回路データ
 4 0 6 F L A S H R O M
 4 0 7 回路データ
 4 0 8 終了通知信号
 4 0 9 保持データ
 4 1 0 出力データ
 5 0 1 暗号復号化装置
 5 0 2 入力データ
 5 0 3 回路データ抽出部
 5 0 4 回路データ
 5 0 5 可変処理回路
 5 0 6 暗号／復号化データ保持部
 5 0 7 終了通知信号
 5 0 8 出力データ
 5 0 9 保持データ
 6 0 1 暗号復号化装置
 6 0 2 入力データ
 6 0 3 暗号／復号化データ保持部
 6 0 4 データ解析部
 6 0 5 F P G A回路データ生成部
 6 0 6 ランダム発生器

607	セレクター	
608, 608a, 608b, 608n	ROM	
609	回路データ	
610	可変処理回路	
611	保持データ	
612	回路変更通知信号	
613	出力データ	
614	解析データ	
615	回路データ	
701	暗号復号化装置	
702	入力データ	
703	暗号／復号化データ保持部	
704	データ解析部	
705	FPGA回路データ生成部	
706	ランダム発生器	
707	セレクター	
708, 708a, 708b, 708n	データ回路部	
709	回路データ	
710	可変処理回路	
711	保持データ	
712	回路変更通知信号	
713	出力データ	
714	解析データ	
715	回路データ	
801	暗号復号化装置	
802	入力データ	
803	暗号／復号化データ保持部	
804	可変処理回路	
805	回路変更通知信号	

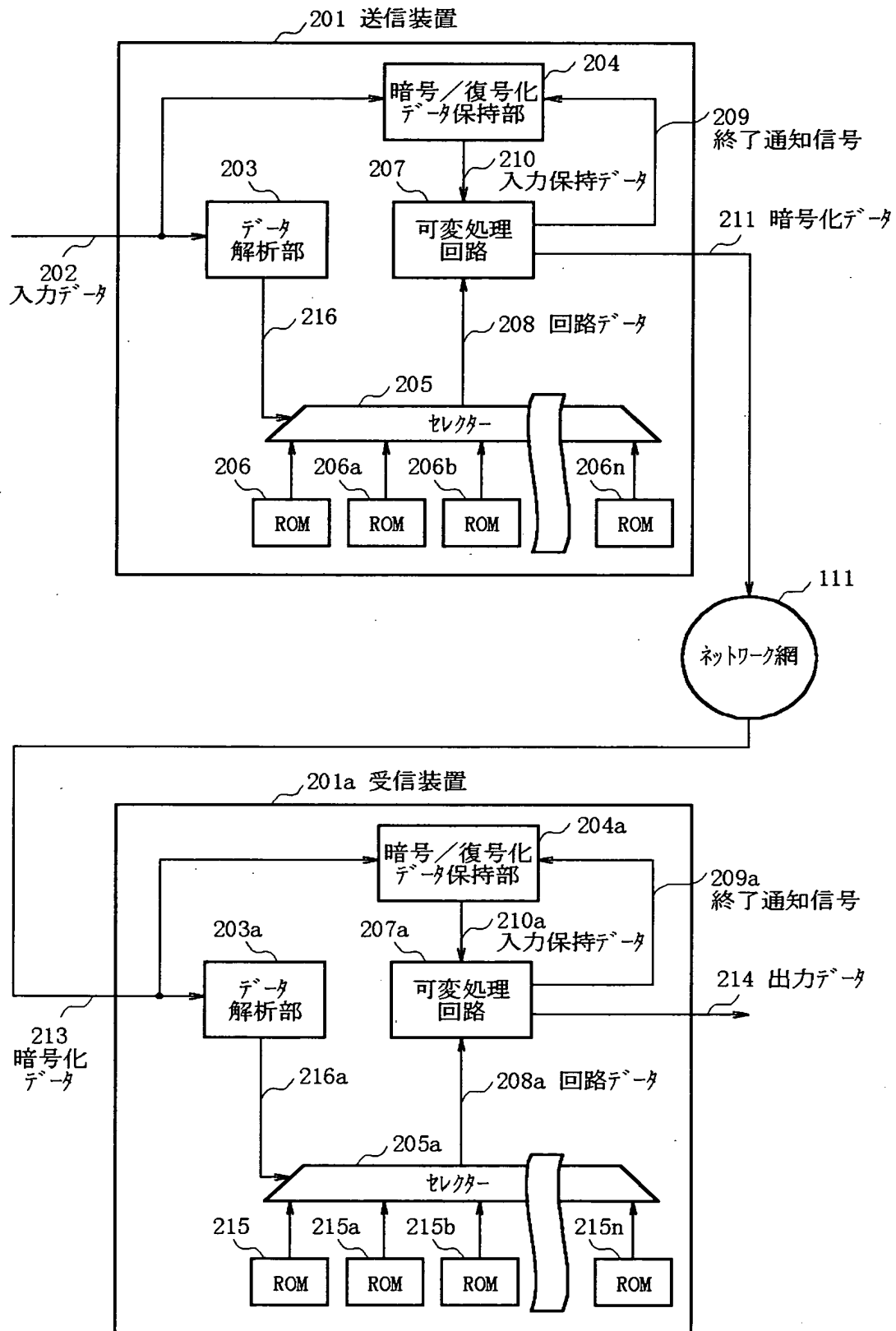
8 0 6	保持データ	
8 0 7	出力データ	
8 0 8	タイマー	
8 0 9	セレクター	
8 1 0, 8 1 0 a, 8 1 0 b, 8 1 0 n	ROM	
8 1 1	回路データ	
8 1 2	セレクター制御信号	
9 0 1	暗号復号化装置	
9 0 2	入力データ	
9 0 3	暗号／復号化データ保持部	
9 0 4	可変処理回路	
9 0 5	回路変更通知信号	
9 0 6	保持データ	
9 0 7	出力データ	
9 0 8	タイマー	
9 0 9	F P G A回路データ生成部	
9 1 0	セレクター	
9 1 1, 9 1 1 a, 9 1 1 b, 9 1 1 n	データ回路部	
9 1 2	回路データ	
9 1 3	回路データ	

【書類名】 図面

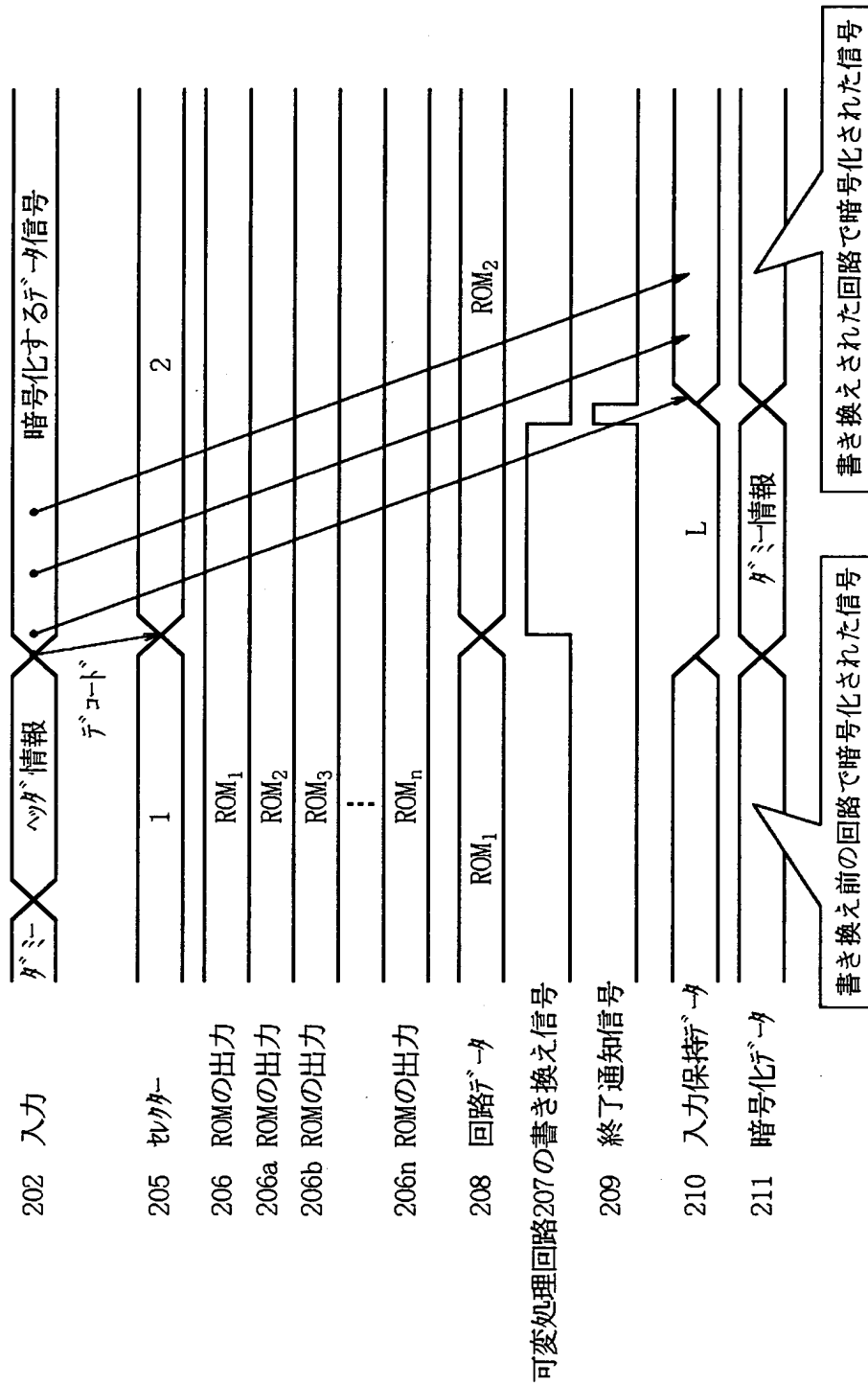
【図 1】



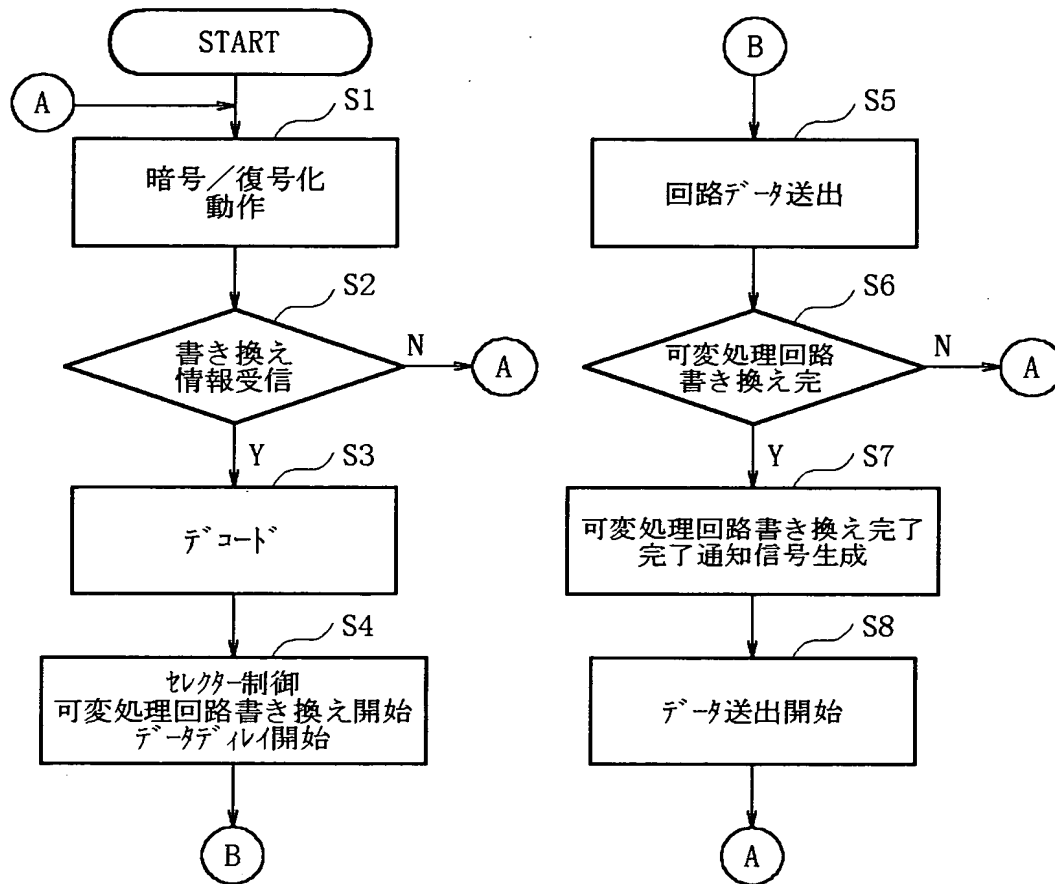
【図 2】



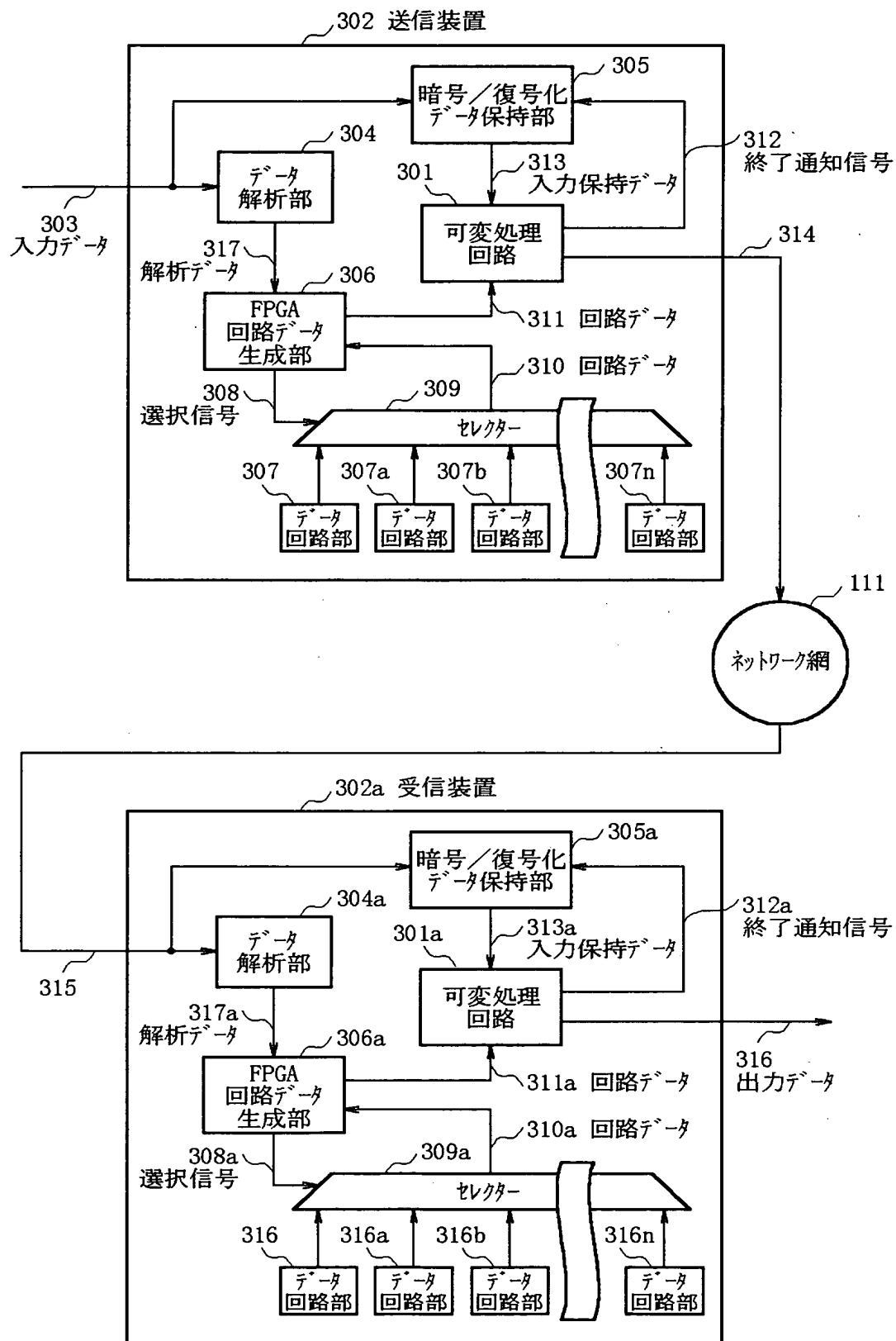
【図 3】



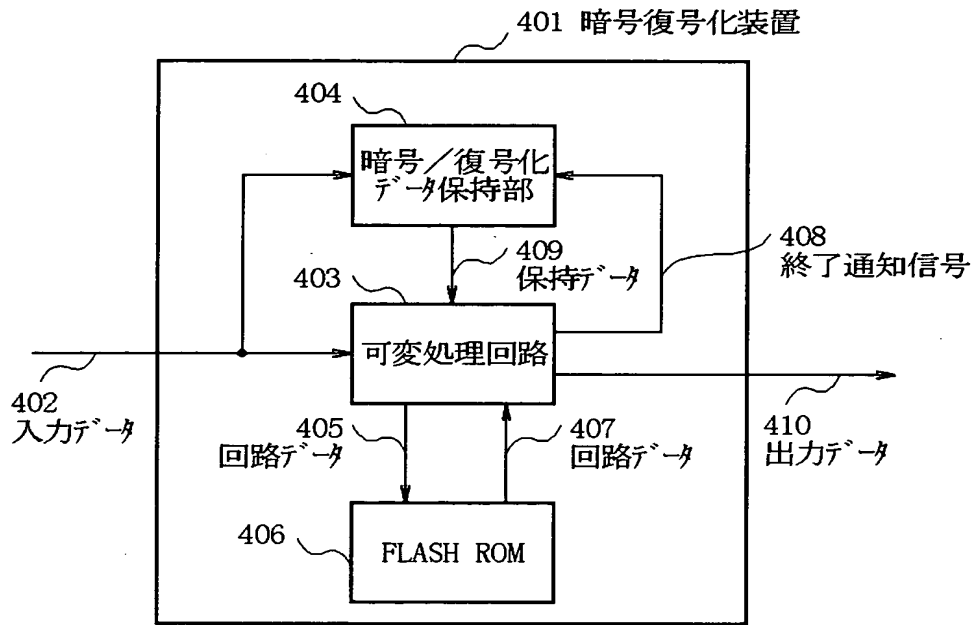
【図 4】



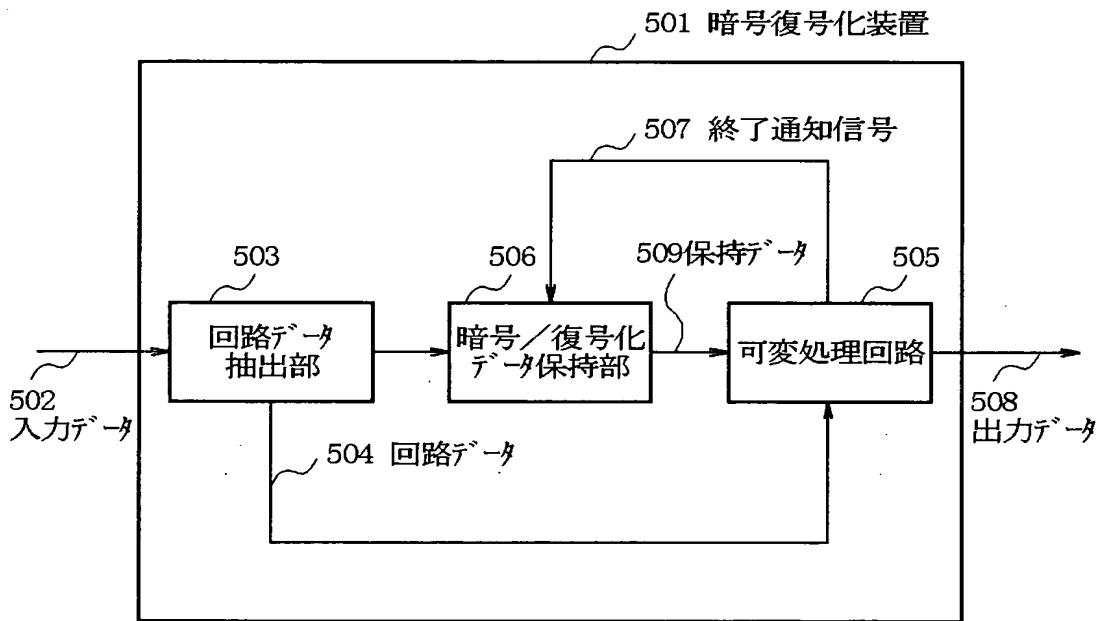
【図 5】



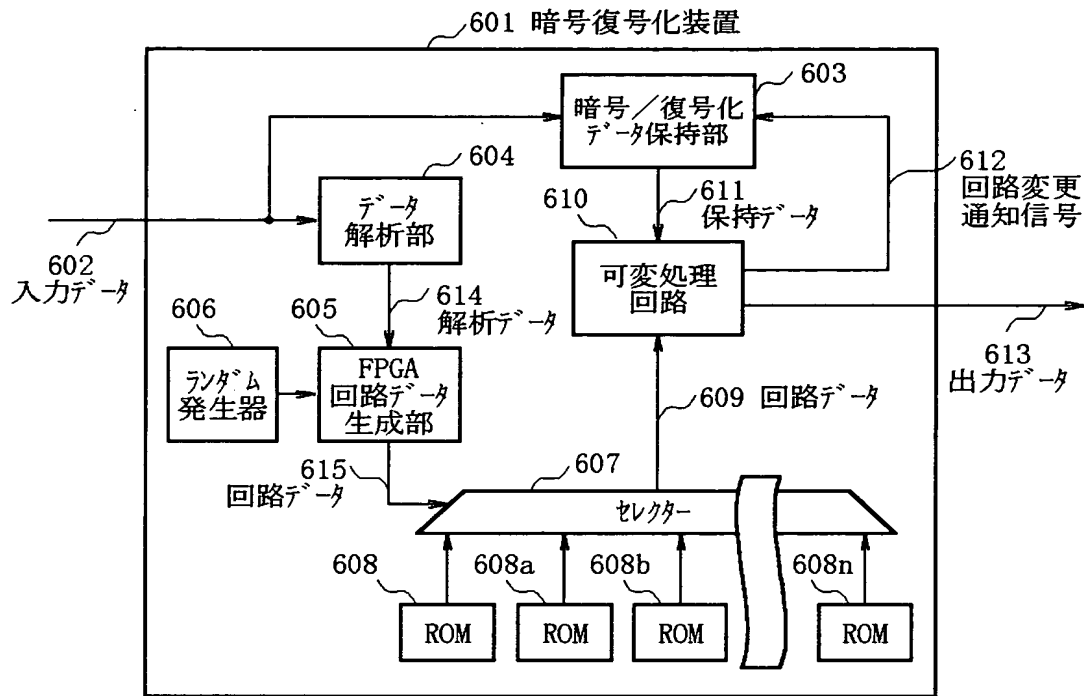
【図 6】



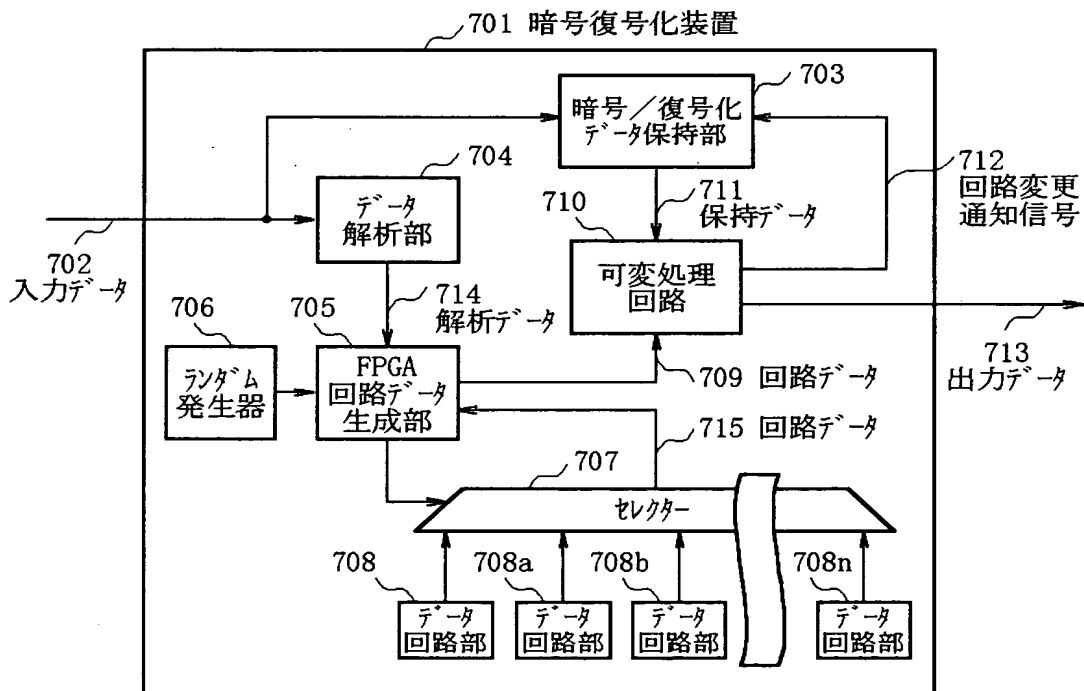
【図 7】



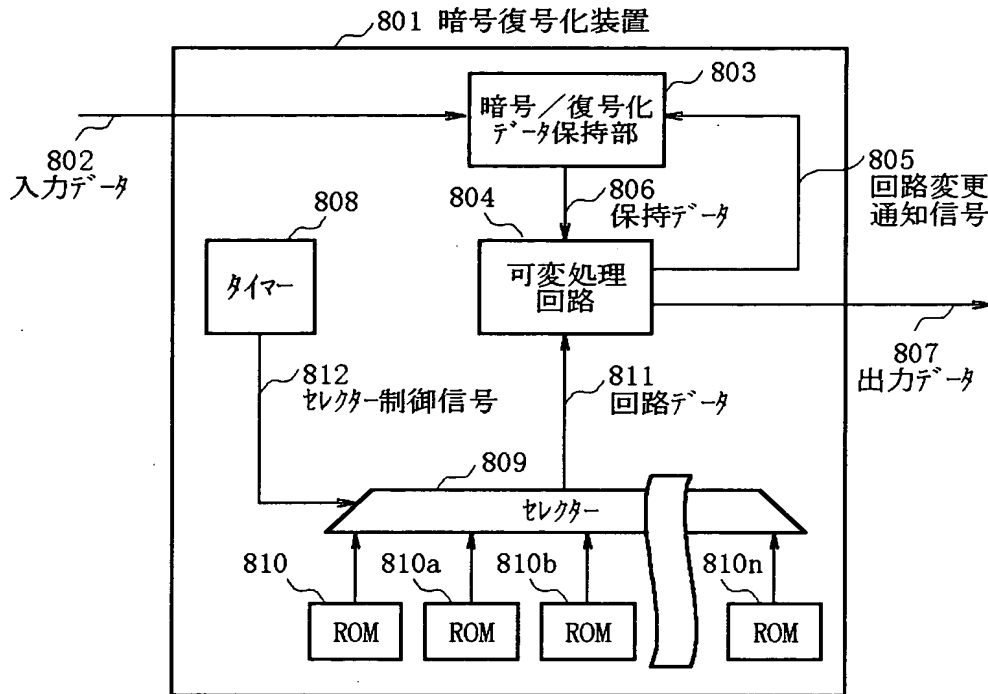
【図 8】



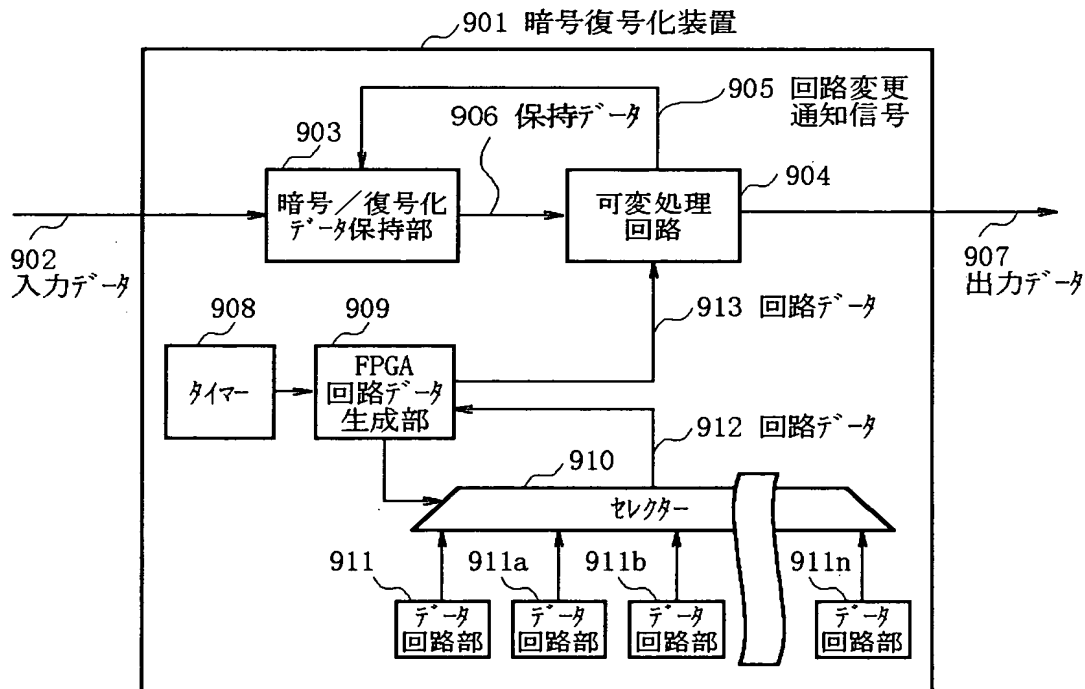
【図 9】



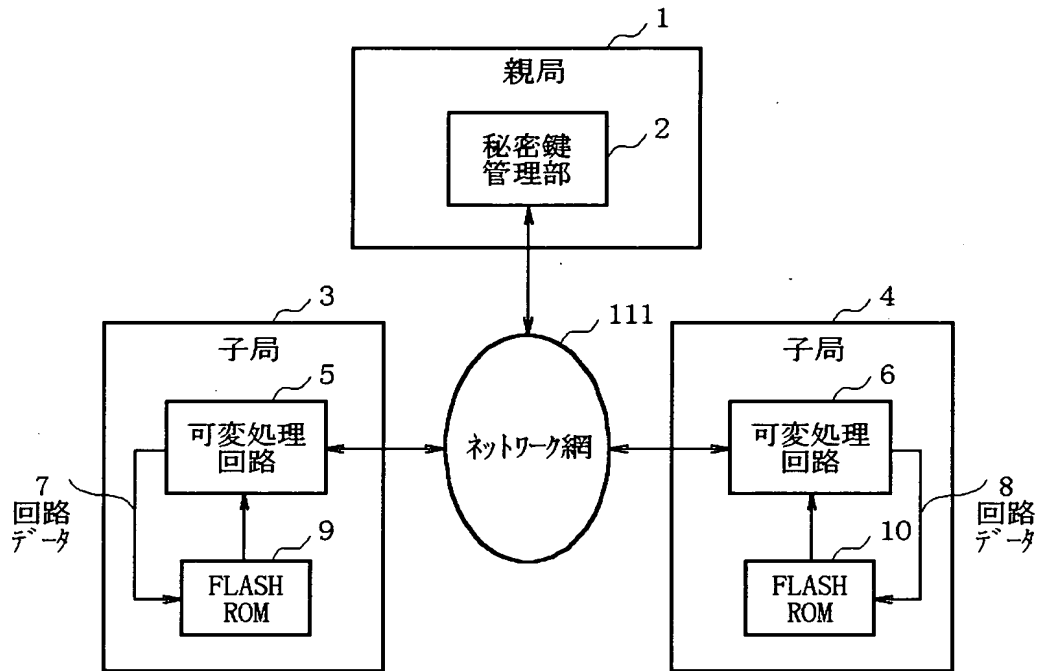
【図 1 0】



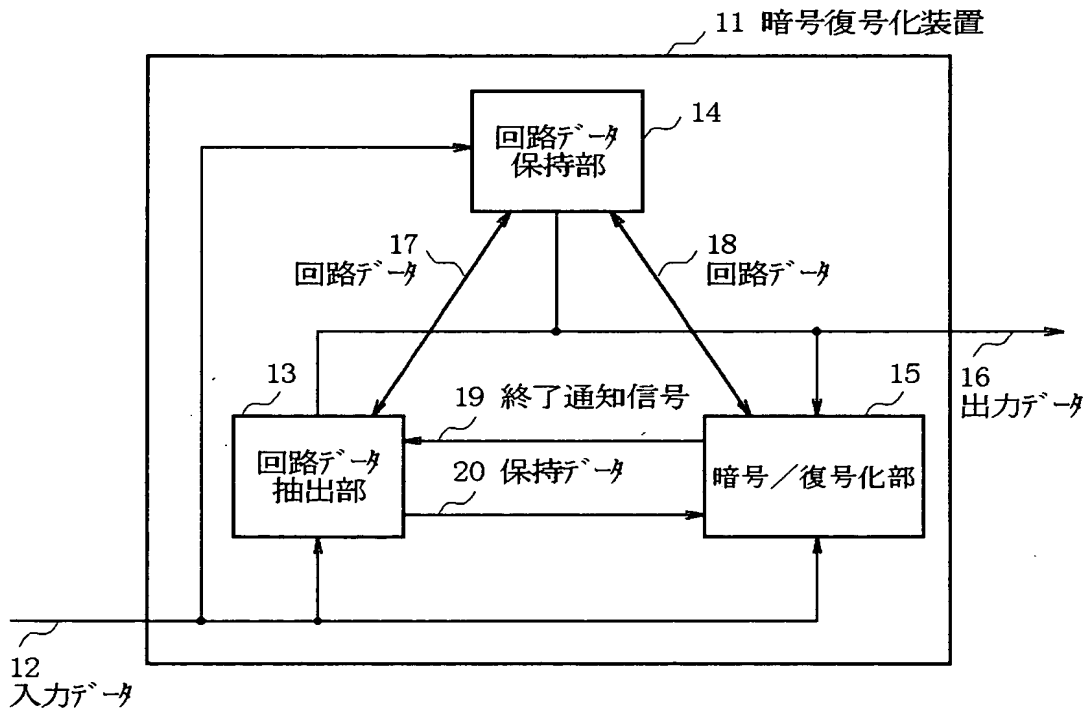
【図 1 1】



【図 1 2】



【図 1 3】



【書類名】 要約書

【要約】

【課題】 暗号復号化方法のアルゴリズム変更に伴うハードウェア変更を可能とし、暗号復号の高速処理を図る。

【解決手段】 送信装置 1 0 2 は入力データ 1 0 1 を暗号化し暗号化データ 1 1 0 を出力する。ネットワーク網 1 1 1 は暗号化データ 1 1 0 を伝送する。受信装置 1 0 6 はネットワーク網 1 1 1 を介して伝送されてきて暗号化データ 1 1 3 を入力し、暗号解読を行い復号化した出力データ 1 1 2 を出力する。

可変処理回路 1 0 3 は入力データ 1 0 1 暗号化する。ROM 1 0 4 は秘密鍵の回路データ 1 0 5 を可変処理回路 1 0 3 に出力する。可変処理回路 1 0 7 は暗号化データ 1 1 3 を復号する。ROM 1 0 8 は秘密鍵の回路データ 1 0 9 を可変処理回路 1 0 7 に出力する。

【選択図】 図 1

認 定 ・ 付 加 情 報

特許出願の番号	特願 2 0 0 0 - 1 1 8 2 6 9
受付番号	5 0 0 0 0 4 9 5 3 1 4
書類名	特許願
担当官	第七担当上席 0 0 9 6
作成日	平成 1 2 年 4 月 2 0 日

< 認定情報・付加情報 >

【提出日】	平成12年 4月19日
-------	-------------

出 願 人 履 歴 情 報

識別番号 [000232254]

1. 変更年月日	1990年 8月30日
[変更理由]	新規登録
住 所	東京都港区三田1丁目4番28号
氏 名	日本電気通信システム株式会社